

20 OCT 2004

10/5/2009/003586

17. 3. 2004

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

2003年 4月 1日

REC'D 29 APR 2004

出願番号  
Application Number:

特願 2003-098596

WIPO PCT

[ST. 10/C]: [JP 2003-098596]

出願人  
Applicant(s):

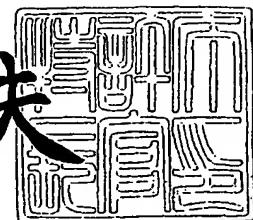
松下電器産業株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 4月 15日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特 2004-3031786

【書類名】 特許願

【整理番号】 2054051019

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

G07C 3/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 吉田 順二

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 ▲浜▼井 信二

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213583

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 サーバ認証装置、認証装置およびダウンロードサーバの運用方法、媒体及び情報集合体

【特許請求の範囲】

【請求項1】 あるアプリケーションサーバが正当であることを保証し認証局が発行するサーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有し、前記認証局が発行するCA情報を、内部に保存するためのメモリと、

前記署名の認証を行うためのダウンロード公開鍵を保存するダウンロード公開鍵用メモリと、

前記認証局に関連するダウンロードサーバに接続し、前記CA情報を前記ダウンロードサーバから取得し、前記メモリに保存するCA情報更新手段と、

前記アプリケーションサーバから前記サーバ証明書を取得し、前記メモリに保存されている前記CA情報内の前記CA証明書で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、

初期状態では、前記メモリには最初の前記CA情報が保存され、

前記CA情報更新手段は、前記CA証明書を更新する必要があれば、前記更新用アドレスが指定する前記ダウンロードサーバから新しいCA情報を取得し、前記CA情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記CA情報が正当であると証明できた場合には、前記CA情報を前記メモリに保存することを特徴とするサーバ認証装置。

【請求項2】 前記ダウンロードサーバは、少なくとも鍵情報を含み、前記メモリに保存されている前記CA情報内の前記CA証明書を用いることで前記ダウンロードサーバが正当であることを証明可能なDLサーバ証明書を保有しており、

前記CA情報更新手段は、前記ダウンロードサーバ接続時に、まず前記DLサーバ証明書を取得し、前記メモリに保存されている前記CA情報内の前記CA証明書で認証を行い、前記DLサーバ証明書の正当性を証明できた場合には、前記

DLサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいCA情報を取得し、

前記CA情報更新手段は、前記DLサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいCA情報の取得を行わないことを特徴とする請求項1記載のサーバ認証装置。

【請求項3】 新しく取得したCA情報に記載されている前記更新用アドレスは、前記CA情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいCA情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする請求項2記載のサーバ認証装置。

【請求項4】 あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するCA情報を、内部に保存するための第1のメモリおよび第2のメモリと、

前記認証局に関連するダウンロードサーバに接続し、前記CA情報を前記ダウンロードサーバから取得し、前記第1のメモリもしくは前記第2のメモリに保存するCA情報更新手段と、

前記アプリケーションサーバから前記サーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、

初期状態では、前記第1のメモリには最初の前記CA情報が保存され、また前記第2のメモリには何も保存されておらず、

前記CA情報更新手段は、ある期間ごとに前記第1のメモリに保存されている前記CA情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードサーバに接続できた場合には、前記ダウンロードサーバから新しいCA情報を取得し、前記新しいCA情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいCA情報が正当であると証明できた場合には、前記新しいCA情報を前記第2のメモリに保存し、

前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記

サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できなかった場合には、前記第1のメモリに保存されている前記CA情報内の前記CA証明書の代わりに、前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の認証を行い、もし前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以前に前記第2のメモリに保存されている前記CA情報を前記サーバ証明書の認証に用い、かつ第1のメモリに保存されている前記CA情報を削除し、以降は前記第1のメモリと、前記第2のメモリの役割を入れ替えて実行することを特徴とするサーバ認証装置。

**【請求項5】** 前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できなかった場合には、前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第2のメモリに保存されている前記CA情報を前記第1のメモリにコピーし、かつ前記第2のメモリに保存されている前記CA情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする請求項4記載のサーバ認証装置。

**【請求項6】** 前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いることで前記ダウンロードサーバが正当であることを証明するDLサーバ証明書を保有しており、

前記CA情報更新手段は、前記ダウンロードサーバ接続時に、まず前記DLサーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記CA証明書で認証を行い、前記DLサーバ証明書の正当性を証明できた場合には、前記DLサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいCA情報を取得し、

前記CA情報更新手段は、前記DLサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいCA情報の取得

を行わないことを特徴とする請求項4または5記載のサーバ認証装置。

【請求項7】 新しく取得したCA情報に記載されている前記更新用アドレスは、前記CA情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいCA情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする請求項6記載のサーバ認証装置。

【請求項8】 あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するCA情報を、内部に保存するための第1のメモリと、

前記認証局に関連するダウンロードサーバに接続し、前記CA情報を前記ダウンロードサーバから取得し、前記第1のメモリに保存するCA情報更新手段と、

前記アプリケーションサーバから前記サーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、

初期状態では、前記第1のメモリには最初の前記CA情報が保存されており、

前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できなかった場合には、前記CA情報更新手段に更新指示を送り、

前記CA情報更新手段は、前記CA情報更新手段から前記更新指示を受け取ると、前記第1のメモリに保存されている前記CA情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードに接続できた場合には、前記ダウンロードサーバから新しいCA情報を取得し、前記新しいCA情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいCA情報が正当であると証明できた場合には、前記新しいCA情報を前記第1のメモリに保存することを特徴とするサーバ認証装置。

【請求項9】 さらに前記CA情報を保存するための第2のメモリを保有し、

前記第2のメモリは、初期状態には何も保存されておらず、

前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記

サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できず、かつ前記第2のメモリに何も保存されていなかつた場合には、前記CA情報更新手段に更新指示を送り、

前記CA情報更新手段は、取得した前記新しいCA情報を前記第1のメモリの代わりに前記第2のメモリに保存し、

前記サーバ証明書認証手段は、前記新しいCA情報が前記第2のメモリに保存されると、前記第2のメモリに保存されている前記新しいCA情報内の前記CA証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第2のメモリに保存されている前記CA情報を前記サーバ証明書の認証に用い、かつ第1のメモリに保存されている前記CA情報を削除し、以降は前記第1のメモリと、前記第2のメモリの役割を入れ替えて実行することを特徴とする請求項8記載のサーバ認証装置。

**【請求項10】** 前記サーバ証明書認証手段は、前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第2のメモリに保存されている前記CA情報を前記第1のメモリにコピーし、かつ前記第2のメモリに保存されている前記CA情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする請求項9記載のサーバ認証装置。

**【請求項11】** 前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いることで前記ダウンロードサーバが正当であることを証明するDLサーバ証明書を保有しております、

前記CA情報更新手段は、前記ダウンロードサーバ接続時に、まず前記DLサーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記CA証明書で認証を行い、前記DLサーバ証明書の正当性を証明できた場合には、前記DLサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいCA情報を取得し、

前記CA情報更新手段は、前記DLサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいCA情報の取得

を行わないことを特徴とする請求項 8 または 9 または 10 記載のサーバ認証装置

。

【請求項 12】 新しく取得した CA 情報に記載されている前記更新用アドレスは、前記 CA 情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しい CA 情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする請求項 11 記載のサーバ認証装置。

【請求項 13】 請求項 1 ~ 12 のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体。

【請求項 14】 請求項 1 ~ 12 のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体。

【請求項 15】 あるアプリケーションサーバが正当であることを保証するサーバ証明書を発行し、かつ前記サーバ証明書が正当であることを認証するための CA 証明書と、次回更新用アドレスと、前記 CA 証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも含み、有効期間を持つ CA 情報を発行し、かつ前記 CA 情報の正当性を証明する前記署名を作成するための DL 秘密鍵を保有する認証局の機能を持つ認証装置と、

保有している前記 CA 情報を用いて前記アプリケーションサーバの前記証明書の正当性を証明するサーバ認証装置からの要求に応じ、前記 CA 情報に前記署名を含めて前記サーバ認証装置に送信するダウンロードサーバとにおける認証装置およびダウンロードサーバの運用方法であって、

有効期間が TC1 であり、かつ次回更新アドレスは第 2 のダウンロードサーバを示すアドレスである第 1 の CA 情報を発行する第 1 の認証装置を稼働させるステップと、

以降、 $N \geq 1$  である整数 N に対し、

第 N の CA 情報の有効期間が終了するより期間 TDN ( $TCN > TDN$ ) だけ前の時点で、有効期間が  $TC(N+1)$  であり、かつ次回更新アドレスは第 (N

+2) のダウンロードサーバを示すアドレスである第(N+1)のCA情報、および前記第(N+1)のCA情報内のCA証明書で認証可能なサーバ証明書を発行する第(N+1)の認証装置を稼働させるステップと、

前記第(N+1)の認証装置の稼働と同時に、前記サーバ認証装置からの要求に応じ、前記第(N+1)のCA情報を前記サーバ認証装置に送信する第(N+1)のダウンロードサーバを稼働させるステップと、

第NのCA情報の有効期間が終了すると、前記第Nの認証装置を終了するステップと

本来の第NのCA情報の有効期間が終了する時点で、前記第(N+1)のダウンロードサーバの稼働を終了するステップとを繰り返す、認証装置およびダウンロードサーバの運用方法。

【請求項16】 さらに、

第NのCA情報の有効期間が残りTDNになる以前に、前記第NのCA情報を無効にする必要が発生し、かつその時点で前記第(N+1)の認証装置および前記第(N+1)のダウンロードサーバが稼働していない場合には、

有効期間をTC(N+1)とし、かつ次回更新アドレスは第(N+2)のダウンロードサーバを示すアドレスである第(N+1)のCA情報を発行する第(N+1)の認証装置をその時点で稼働させるステップと、

第(N+1)の認証装置の稼働と同時に前記第(N+1)のCA情報を前記サーバ認証装置に送信する第(N+1)のダウンロードサーバを稼働させるステップと、

第(N+1)の認証装置の稼働と同時に前記第Nの認証装置の稼働を終了し、前記第NのCA情報を無効にするステップとを実行し、

第NのCA情報の有効期間が残りTDNになる以前に、前記第NのCA情報を無効にする必要が発生し、かつ前記第(N+1)の認証装置および前記第(N+1)のダウンロードサーバがすでに稼働している場合には、

その時点で前記第Nの認証装置の稼働を終了し、前記第NのCA情報を無効にするステップとを実行することを特徴とする請求項15記載の認証装置およびダウンロードサーバの運用方法。

**【請求項 17】** 前記第Nのダウンロードサーバは、少なくとも第Nの鍵情報を含み、前記第Nのダウンロードサーバが正当であることを証明する第NのDLサーバ証明書を保有しており、かつ前記サーバ認証装置の要求に応じて前記第NのDLサーバ証明書を送信し、

かつ前記第Nの鍵情報を用いた秘密通信によって、前記サーバ認証装置に第NのCA情報を送信することを特徴とする請求項15または請求項16に記載の認証装置およびダウンロードサーバの運用方法。

#### 【発明の詳細な説明】

##### 【0001】

###### 【発明の属する技術分野】

本発明は、認証局によって発行されるサーバ証明書の正当性を認証するためのCA情報が有効期間切れなどのために失効する場合に、安全かつ確実に新しいCA情報を更新できるサーバ認証装置、認証局およびダウンロードサーバの運用方法、媒体及び情報集合体に関するものである。

##### 【0002】

###### 【従来の技術】

近年、インターネットは急速に普及、拡大し、電子メールやインターネットショッピングなど様々なサービスが提供されている。しかし、その一方で個人情報など、インターネットを通して通信されるデータの盗聴や改ざんなどの問題も発生してきた。こうした悪意ある第3者からの攻撃を防ぐために、様々なセキュリティ技術が考案、導入されてきた。セキュリティ技術としては、例えば通信データが途中で盗聴されても内容を分からないようにする暗号や、通信データが途中で改ざんされていないかを検証できる認証などが挙げられる。

##### 【0003】

こうした技術を利用し、インターネットでよく用いられているセキュリティ技術にSSL (Secure Sockets Layer) と呼ばれる方式がある。SSLは、特許文献1で提案されており、サーバが正当であること、通信において通信データの内容が漏洩していないこと、かつ受信するクライアントが受け取った通信データの内容が途中で改ざんされていないことの3つを保証する通

信を提供する方式である。

#### 【0004】

SSLにおける通信方式の概要を、図8および図9を用いて説明する。

#### 【0005】

図8は、SSLにおける鍵情報および証明書の準備を表す図である。図8において、101は認証局、102はクライアント、103はサーバ、104はCA公開鍵、105はCA秘密鍵、106はCA証明書、107はサーバ公開鍵、108はサーバ秘密鍵、109はサーバ証明書、110は署名である。

#### 【0006】

図9は、SSLにおける通信プロトコルを表す図である。図9において、201は通信共通鍵である。

#### 【0007】

認証局101は、あらかじめCA公開鍵104とCA秘密鍵105のペアを生成し、同時にCA公開鍵104や認証局101に関する情報を記載したCA証明書106を作成する。

#### 【0008】

サーバ103は、稼働前にまずサーバ公開鍵107とサーバ秘密鍵のペアを生成する。サーバ103は、サーバ公開鍵107とサーバ103に関する情報を認証局101に送信し、サーバ証明書109の発行を依頼する。

#### 【0009】

認証局101は、CA秘密鍵105を用いて、サーバ103から受け取った情報やその他必要な情報から署名110を作成し、サーバ103から受け取った情報やその他必要な情報および署名110を合わせたものをサーバ証明書109として、サーバ103に発行する。

#### 【0010】

サーバ103は受け取ったサーバ証明書109を保存しておく。

#### 【0011】

またクライアント102は、あらかじめ認証局101からCA証明書106を取得し、保存しておく。

**【0012】**

実際にクライアント102とサーバ103の間で秘密通信は以下のように行われる。

**【0013】**

クライアント102はサーバ103に接続すると、まず秘密通信で用いる暗号化方式の仕様を相互に確認する。

**【0014】**

次にサーバ103はクライアント102にサーバ証明書109を送付する。

**【0015】**

クライアント102は、内部に保存しているCA公開鍵104を用いてサーバ証明書109が正当であるかどうかを確認する。もしサーバ証明書109が正当、すなわちサーバ証明書109に含まれている署名110がCA秘密鍵105で署名されたものであれば、クライアント102はCA公開鍵104を用いて検証すれば、サーバ証明書109が正当であることが確認できる。

**【0016】**

クライアント102は、サーバ証明書109が正当であると確認すると、クライアント側共通鍵生成情報をランダムに作成し、サーバ103に送付する。

**【0017】**

サーバ103は、サーバ側共通鍵生成情報をランダムに作成し、クライアント102に送付する。

**【0018】**

サーバ103およびクライアント102は、サーバ側共通鍵生成情報およびクライアント側共通鍵生成情報を用いて、通信用共通鍵201を生成する。

**【0019】**

これにより、クライアント102とサーバ103で通信用共通鍵201を共有することができる。

**【0020】**

以降、クライアント102およびサーバ103は、通信用共通鍵201を用いて、通信するデータの暗号化および復号を行うことで、秘密通信を行うことが可

能となる。

#### 【0021】

なお、CA証明書106やサーバ証明書109のフォーマットとしては、ITU-T（国際電気通信連合）で定義されたX.509証明書を用いることが多い。

#### 【0022】

さて、X.509証明書においては、サーバ証明書109には有効期限を設けるようになっている。というのも、秘密鍵の安全性は、公開鍵や通信データから秘密鍵を計算するときにかかる時間が十分に長いことに依存しており、同じ鍵を長期間使用していると、その分秘密鍵が暴露される可能性が高くなるためである。

#### 【0023】

同様にCA証明書106にも有効期限を設けるが、一般にサーバ証明書109より長い期間が設定されている。

#### 【0024】

ところで、CA証明書の有効期限が切れた場合、もしくは何らかの原因でCA秘密鍵が暴露されてしまった場合には、速やかに新しい鍵ペアを作成し、新しいCA証明書を発行もしくは取得しなければならない。

#### 【0025】

例えば、十分な数の認証局が同時に存在し、クライアントがPC（パーソナルコンピュータ）のように、十分な計算機リソースを保有しており、それらのCA証明書を全てもしくは十分な数だけ保有可能な場合は、サーバは失効した認証局の代わりに別の認証局から取得したサーバ証明書を使用することが可能である。クライアントは、保有しているCA証明書を順番に用いてサーバ証明書の認証を行い、いずれかのCA証明書でサーバ証明書の正当性を確認できれば、そのサーバは正当であると確認できる。

#### 【0026】

また新しい認証局ができ、そのCA証明書を取得するためには、例えば認証局自身もしくは信頼できるサーバなどから、クライアントのユーザが取得し、ユ

ーザが自分でクライアントにインストールするなどして実行できる。

#### 【0027】

またサーバ証明書の有効期限が間近になった場合や、サーバ証明書が失効した場合に、自動的に新しいサーバ証明書を更新する装置および方法が、例えば特許文献2や特許文献3に記載されている。

#### 【0028】

##### 【特許文献1】

U. S. Patent 5657390

#### 【0029】

##### 【特許文献2】

特開2001-197054号公報

#### 【0030】

##### 【特許文献3】

特開2002-215826号公報

#### 【0031】

##### 【発明が解決しようとする課題】

しかしながら、家電製品などのように十分なリソースを保有していないクライアントの場合には、常に多数個のCA証明書を保有したり、複数のCA証明書を用いて検証するプログラムもしくは回路を組み込むことが困難であるという問題点が生じる。

#### 【0032】

また、時計を保有していないなかったり、あるいは時計を正確な時刻に設定する手段を持たないクライアントの場合には、CA証明書の有効期限の判定が困難で、有効期限が近づくと新しいCA証明書を自動的に更新することができないという問題点がある。

#### 【0033】

本発明は、このような従来の問題点を鑑みてなされたものであって、リソースが少ないクライアントであっても、安全かつ確実にCA証明書を更新することができるサーバ認証装置、認証局およびダウンロードサーバの運用方法、媒体及び

情報集合体を提供することを目的とするものである。

### 【0034】

#### 【課題を解決するための手段】

上述した課題を解決するために、第1の本発明（請求項1に対応）は、あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有し、前記認証局が発行するCA情報を、内部に保存するためのメモリと、前記署名の認証を行うためのダウンロード公開鍵を保存するダウンロード公開鍵用メモリと、前記認証局に関連するダウンロードサーバに接続し、前記CA情報を前記ダウンロードサーバから取得し、前記メモリに保存するCA情報更新手段と、前記アプリケーションサーバから前記サーバ証明書を取得し、前記メモリに保存されている前記CA情報内の前記CA証明書で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、初期状態では、前記メモリには最初の前記CA情報が保存され、前記CA情報更新手段は、前記CA証明書を更新する必要があれば、前記更新用アドレスが指定する前記ダウンロードサーバから新しいCA情報を取得し、前記CA情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記CA情報が正当であると証明できた場合には、前記CA情報を前記メモリに保存することを特徴とするサーバ認証装置である。

### 【0035】

第2の本発明（請求項2に対応）は、前記ダウンロードサーバは、少なくとも鍵情報を含み、前記メモリに保存されている前記CA情報内の前記CA証明書を用いることで前記ダウンロードサーバが正当であることを証明可能なDLサーバ証明書を保有しており、前記CA情報更新手段は、前記ダウンロードサーバ接続時に、まず前記DLサーバ証明書を取得し、前記メモリに保存されている前記CA情報内の前記CA証明書で認証を行い、前記DLサーバ証明書の正当性を証明できた場合には、前記DLサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいCA情報を取得し、前記CA情報更新手段は、前記DLサーバ証明書の正当性を証明できなかった場

合には前記ダウンロードサーバとの接続を中断し、前記新しいCA情報の取得を行わないことを特徴とする第1の本発明に記載のサーバ認証装置である。

### 【0036】

第3の本発明（請求項3に対応）は、新しく取得したCA情報に記載されている前記更新用アドレスは、前記CA情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいCA情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする第2の本発明に記載のサーバ認証装置である。

### 【0037】

第4の本発明（請求項4に対応）は、あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するCA情報を、内部に保存するための第1のメモリおよび第2のメモリと、前記認証局に関連するダウンロードサーバに接続し、前記CA情報を前記ダウンロードサーバから取得し、前記第1のメモリもしくは前記第2のメモリに保存するCA情報更新手段と、前記アプリケーションサーバから前記サーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、初期状態では、前記第1のメモリには最初の前記CA情報が保存され、また前記第2のメモリには何も保存されておらず、前記CA情報更新手段は、ある期間ごとに前記第1のメモリに保存されている前記CA情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードサーバに接続できた場合には、前記ダウンロードサーバから新しいCA情報を取得し、前記新しいCA情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいCA情報が正当であると証明できた場合には、前記新しいCA情報を前記第2のメモリに保存し、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できなかった場合には、前記第1のメモリに保存されている前記CA情報内の

前記CA証明書の代わりに、前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の認証を行い、もし前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第2のメモリに保存されている前記CA情報を前記サーバ証明書の認証に用い、かつ第1のメモリに保存されている前記CA情報を削除し、以降は前記第1のメモリと、前記第2のメモリの役割を入れ替えて実行することを特徴とするサーバ認証装置である。

### 【0038】

第5の本発明（請求項5に対応）は、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できなかった場合には、前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第2のメモリに保存されている前記CA情報を前記第1のメモリにコピーし、かつ前記第2のメモリに保存されている前記CA情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする第4の本発明に記載のサーバ認証装置である。。

### 【0039】

第6の本発明（請求項6に対応）は、前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いることで前記ダウンロードサーバが正当であることを証明するDLサーバ証明書を保有しており、前記CA情報更新手段は、前記ダウンロードサーバ接続時に、まず前記DLサーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記CA証明書で認証を行い、前記DLサーバ証明書の正当性を証明できた場合には、前記DLサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいCA情報を取得し、前記CA情報更新手段は、前記DLサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいCA情報の取得を行わないことを特徴とする第4または第5の本発明に記載のサーバ認証装置である。

## 【0040】

第7の本発明（請求項7に対応）は、新しく取得したCA情報に記載されている前記更新用アドレスは、前記CA情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいCA情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする第6の本発明に記載のサーバ認証装置である。

## 【0041】

第8の本発明（請求項8に対応）は、あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するCA情報を、内部に保存するための第1のメモリと、前記認証局に関連するダウンロードサーバに接続し、前記CA情報を前記ダウンロードサーバから取得し、前記第1のメモリに保存するCA情報更新手段と、前記アプリケーションサーバから前記サーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、初期状態では、前記第1のメモリには最初の前記CA情報が保存されており、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できなかった場合には、前記CA情報更新手段に更新指示を送り、前記CA情報更新手段は、前記CA情報更新手段から前記更新指示を受け取ると、前記第1のメモリに保存されている前記CA情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードに接続できた場合には、前記ダウンロードサーバから新しいCA情報を取得し、前記新しいCA情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいCA情報が正当であると証明できた場合には、前記新しいCA情報を前記第1のメモリに保存することを特徴とするサーバ認証装置である。

## 【0042】

第9の本発明（請求項9に対応）は、さらに前記CA情報を保存するための第

2のメモリを保有し、前記第2のメモリは、初期状態には何も保存されておらず、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いて正しく認証できず、かつ前記第2のメモリに何も保存されていなかつた場合には、前記CA情報更新手段に更新指示を送り、前記CA情報更新手段は、取得した前記新しいCA情報を前記第1のメモリの代わりに前記第2のメモリに保存し、前記サーバ証明書認証手段は、前記新しいCA情報が前記第2のメモリに保存されると、前記第2のメモリに保存されている前記新しいCA情報内の前記CA証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第2のメモリに保存されている前記CA情報を前記サーバ証明書の認証に用い、かつ第1のメモリに保存されている前記CA情報を削除し、以降は前記第1のメモリと、前記第2のメモリの役割を入れ替えて実行することを特徴とする第8の本発明に記載のサーバ認証装置である。

#### 【0043】

第10の本発明（請求項10に対応）は、前記サーバ証明書認証手段は、前記第2のメモリに保存されている前記CA情報内の前記CA証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第2のメモリに保存されている前記CA情報を前記第1のメモリにコピーし、かつ前記第2のメモリに保存されている前記CA情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする第9の本発明に記載のサーバ認証装置である。

#### 【0044】

第11の本発明（請求項11に対応）は、前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第1のメモリに保存されている前記CA情報内の前記CA証明書を用いることで前記ダウンロードサーバが正当であることを証明するDLサーバ証明書を保有しており、前記CA情報更新手段は、前記ダウンロードサーバ接続時に、まず前記DLサーバ証明書を取得し、前記第1のメモリに保存されている前記CA情報内の前記CA証明書で認証を行い、前記DLサーバ証明書の正当性を証明できた場合には、前記DLサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいCA

情報を取得し、前記CA情報更新手段は、前記DLサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいCA情報の取得を行わないことを特徴とする第8から第10のいずれかの本発明に記載のサーバ認証装置である。

#### 【0045】

第12の本発明（請求項12に対応）は、新しく取得したCA情報に記載されている前記更新用アドレスは、前記CA情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいCA情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする第11の本発明に記載のサーバ認証装置である。

#### 【0046】

第13の本発明（請求項13に対応）は、第1から第12の本発明のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを持たした媒体であって、コンピュータにより処理可能なことを特徴とする媒体である。

#### 【0047】

第14の本発明（請求項14に対応）は、第1から第12の本発明のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体である。

#### 【0048】

第15の本発明（請求項15に対応）は、あるアプリケーションサーバが正当であることを保証するサーバ証明書を発行し、かつ前記サーバ証明書が正当であることを認証するためのCA証明書と、次回更新用アドレスと、前記CA証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも含み、有効期間を持つCA情報を発行し、かつ前記CA情報の正当性を証明する前記署名を作成するためのDL秘密鍵を保有する認証局の機能を持つ認証装置と、保有している前記CA情報を用いて前記アプリケーションサーバの前記証明書の正当性を証明するサーバ認証装置からの要求に応じ、前記CA情報に前記署名を含めて前記サー

バ認証装置に送信するダウンロードサーバとにおける認証装置およびダウンロードサーバの運用方法であって、有効期間がTC1であり、かつ次回更新アドレスは第2のダウンロードサーバを示すアドレスである第1のCA情報を発行する第1の認証装置を稼働させるステップと、以降、 $N \geq 1$ である整数Nに対し、第NのCA情報の有効期間が終了するより期間TDN (TCN > TDN) だけ前の時点で、有効期間がTC (N+1) であり、かつ次回更新アドレスは第(N+2)のダウンロードサーバを示すアドレスである第(N+1)のCA情報、および前記第(N+1)のCA情報内のCA証明書で認証可能なサーバ証明書を発行する第(N+1)の認証装置を稼働させるステップと、前記第(N+1)の認証装置の稼働と同時に、前記サーバ認証装置からの要求に応じ、前記第(N+1)のCA情報を前記サーバ認証装置に送信する第(N+1)のダウンロードサーバを稼働させるステップと、第NのCA情報の有効期間が終了すると、前記第Nの認証装置を終了するステップと、本来の第NのCA情報の有効期間が終了する時点で、前記第(N+1)のダウンロードサーバの稼働を終了するステップとを繰り返す、認証装置およびダウンロードサーバの運用方法である。

#### 【0049】

第16の本発明（請求項16に対応）は、さらに、第NのCA情報の有効期間が残りTDNになる以前に、前記第NのCA情報を無効にする必要が発生し、かつその時点で前記第(N+1)の認証装置および前記第(N+1)のダウンロードサーバが稼働していない場合には、有効期間をTC (N+1) とし、かつ次回更新アドレスは第(N+2)のダウンロードサーバを示すアドレスである第(N+1)のCA情報を発行する第(N+1)の認証装置をその時点で稼働させるステップと、第(N+1)の認証装置の稼働と同時に前記第(N+1)のCA情報を前記サーバ認証装置に送信する第(N+1)のダウンロードサーバを稼働させるステップと、第(N+1)の認証装置の稼働と同時に前記第Nの認証装置の稼働を終了し、前記第NのCA情報を無効にするステップとを実行し、第NのCA情報の有効期間が残りTDNになる以前に、前記第NのCA情報を無効にする必要が発生し、かつ前記第(N+1)の認証装置および前記第(N+1)のダウンロードサーバがすでに稼働している場合には、その時点で前記第Nの認証装置の

稼働を終了し、前記第NのCA情報を無効にするステップとを実行することを特徴とする第15の本発明に記載の認証装置およびダウンロードサーバの運用方法である。

### 【0050】

第17の本発明（請求項17に対応）は、前記第Nのダウンロードサーバは、少なくとも第Nの鍵情報を含み、前記第Nのダウンロードサーバが正当であることを証明する第NのDLサーバ証明書を保有しており、かつ前記サーバ認証装置の要求に応じて前記第NのDLサーバ証明書を送信し、かつ前記第Nの鍵情報を用いた秘密通信によって、前記サーバ認証装置に第NのCA情報を送信することを特徴とする第15または第16の本発明に記載の認証装置およびダウンロードサーバの運用方法。

### 【0051】

#### 【発明の実施の形態】

以下に、本発明の実施の形態を図面を参照して説明する。

### 【0052】

#### （第1の実施の形態）

以下、本発明の第1の実施の形態について、図1および図2を用いて説明する。

図1は、CA情報の一例である。図1において、301はCA情報、302は次回ダウンロードサーバのURL、303はCA署名である。

### 【0053】

図2は、サーバ認証を行うクライアントの構成例である。図2において、101aは認証局A、101bは認証局B、105aはCA秘密鍵A、105bはCA秘密鍵B、106aはCA証明書A、106bはCA証明書B、301aはCA情報A、301bはCA情報B、302bはダウンロードサーバBのURL、302cはダウンロードサーバCのURL、303aはCA署名A、303bはCA署名B、401はアプリケーションサーバ、402aはAPサーバ証明書A、403aはAPサーバ公開鍵A、404aはAPサーバ秘密鍵A、405aはAP署名A、406bはダウンロードサーバB、408bはDLサーバ証明書B

、409bはDLサーバ公開鍵B、410bはDLサーバ秘密鍵B、412bはDL署名B、413はDL秘密鍵、414はDL公開鍵、415はクライアント、416はサーバ認証部、417はCA情報更新部、418はメモリ、419は予備メモリである。

#### 【0054】

本実施の形態においては、CA情報301を発行し、かつアプリケーションサーバ401にAPサーバ証明書を発行する装置を、認証局と表記する。

#### 【0055】

クライアント415に渡す情報として、CA情報301を用意する。CA情報301には、図1に示すように、CA証明書106、CA証明書106の長さ、将来稼働し次回CA情報をダウンロードするためのダウンロードサーバのURL302、ダウンロードサーバのURLの長さ、CA署名303が含まれている。CA署名303は、CA署名303以外の4つの情報に対して、DL秘密鍵413で署名を行ったものである。DL秘密鍵413は、DL公開鍵414とペアであり、DL公開鍵414を用いることでCA署名303の正当性を調べることができる。

#### 【0056】

以下、クライアント415におけるサーバ認証動作について説明する。

まずアプリケーションサーバ401は、SSL通信用の鍵ペアであるAPサーバ秘密鍵A404aとAPサーバ公開鍵A403aを作成し、APサーバ公開鍵A403aおよびその他の必要事項を認証局A101aに送付し、サーバ証明書の発行を依頼する。

#### 【0057】

認証局A101aは、あらかじめCA秘密鍵A105aとCA公開鍵Aの鍵ペアを保有しており、アプリケーションサーバ401からサーバ証明書の発行依頼を受け取ると、CA秘密鍵A105aによる署名と共にAPサーバ証明書402aを発行し、アプリケーションサーバ401に送付する。

#### 【0058】

また認証局A101aは、CA公開鍵Aを含むサーバ証明書であるCA証明書

A106aを作成し、同時にCA証明書A106aを含むCA情報A301aを作成する。CA情報A301aに付加するURL302bは、ダウンロードサーバB406bのURLである。

#### 【0059】

クライアント415は、初期状態として、内部のメモリ418にCA情報A301aを保存しており、予備メモリ419には何も保存していない。

#### 【0060】

クライアント415がアプリケーションサーバ401とSSL通信を行う場合には、サーバ認証部416はアプリケーションサーバ401からAPサーバ証明書402aを取得し、メモリ418に保存しているCA証明書A106a内のCA公開鍵Aで認証を行うことができる。

#### 【0061】

APサーバ証明書402aが正当であると証明されると、従来の技術で説明したように、クライアント415とアプリケーションサーバ401との間でSSL通信を行うことができるようになる。

#### 【0062】

次に、クライアント415におけるCA情報の更新動作について説明する。

#### 【0063】

CA証明書A106aの有効期限が近づくと、クライアント415があらかじめ新しいCA証明書を取得できるようにする必要がある。そのため、まずCA証明書A106aの有効期限が来る前に、CA秘密鍵B105bとCA公開鍵Bの鍵ペアを持つ新しい認証局B101bを立ち上げ、認証局B101bはCA公開鍵Bを含む新しいCA証明書B106bを作成する。ただしこの時点では、認証局B101bはアプリケーションサーバ401に対するAPサーバ証明書を発行しない。サーバ証明書を発行する場合には、この時点ではアプリケーションサーバ401は、クライアント415とのサーバ認証には、認証局B101bから取得したAPサーバ証明書は使用しない。

#### 【0064】

また認証局B101bは同時にCA証明書B106bから新しいCA情報B3

01bを作成する。内部に記載するURL302cは、次回に新しいCA情報をダウンロードするためのダウンロードサーバCのURLであり、CA署名B303bはCA署名A303aと同様に作成したものである。

#### 【0065】

次に、URL302bで指定される場所にダウンロードサーバB406bを立ち上げ、CA情報B301bをダウンロードできるようにする。このとき、ダウンロードサーバB406bにおいても、DLサーバ公開鍵409bとDLサーバ秘密鍵410bの鍵ペアを生成し、DLサーバ公開鍵409bおよび必要事項を認証局A101aに送付し、認証局A101aからサーバ証明書としてDLサーバ証明書B408bを取得する。

#### 【0066】

さて、クライアント415のCA情報更新部417は、メモリ418に保存しているCA情報A301aに記載されているURL302bが示すダウンロードサーバにある程度の期間、例えば1ヶ月毎に接続を試みる。ダウンロードサーバB406bが稼働していないときには、CA情報更新部417はダウンロードサーバB406bへの接続に失敗するので、この場合には更新する必要はないと判断する。その後1ヶ月後に同様に接続を試みる。

#### 【0067】

またダウンロードサーバB406bが稼働しているときには、CA情報更新部417はダウンロードサーバB406bへの接続に成功するので、まずDLサーバ証明書B408bを取得し、メモリ418に保存しているCA公開鍵Aを用いて認証を行う。

#### 【0068】

DLサーバ証明書B408bの正当性が確認されると、次にCA情報更新部417はダウンロードサーバB406bからCA情報B301bを取得する。CA情報更新部417は、取得したCA情報B301b内のCA署名B303bをDL公開鍵414で認証し、CA情報B301bの正当性を確認できると、CA署名B303bを予備メモリ419に保存する。

#### 【0069】

次にCA証明書106aの有効期限が切れたときのアプリケーションサーバ401とクライアント415の動作について説明する。

#### 【0070】

アプリケーションサーバ401は、CA証明書106aの有効期限が切れる前か、もしくは切れると同時に、APサーバ公開鍵とAPサーバ秘密鍵の新しい鍵ペアを生成し、認証局B101bから新しいAPサーバ証明書Bを取得する。アプリケーションサーバ401は、CA証明書106aの有効期限が切れると、古いAPサーバ証明書A402aを廃棄し、それ以降SSL通信を行う場合には、サーバ証明書としてAPサーバ証明書Bを送付する。

#### 【0071】

このようにCA証明書A106aの有効期限が切れると、クライアント415のサーバ認証部416は、アプリケーションサーバ401との通信にあたり、新しいAPサーバ証明書Bを受け取ることになる。しかし、メモリ418に保存しているCA証明書A106a内のCA公開鍵Aでは、APサーバ証明書Bの認証に失敗する。このときサーバ認証部416は、予備メモリ419に保存されているCA情報B106b内のCA公開鍵Bを用いてAPサーバ証明書Bの認証を行い、APサーバ証明書Bの正当性を確認できると、クライアント415はアプリケーションサーバ401とのSSL通信を継続する。

#### 【0072】

同時に、サーバ認証部416は、予備メモリ419に保存されているCA情報B106bをメモリ418に保存し、予備メモリ419を空にする。これ以降は、サーバ認証部416は、メモリ418に保存されたCA情報106bをアプリケーションサーバ401との認証に用いる。

#### 【0073】

もしこのとき予備メモリ419には何も保存されていない場合には、サーバ認証部416は、CA情報更新部417に新しいCA情報の取得を指示する。

#### 【0074】

CA情報更新部417は、サーバ認証部416から新しいCA情報の取得を指示された場合には、ダウンロードサーバB406bから新しいCA情報B301

bを、上記と同様の手順で取得する。

#### 【0075】

サーバ認証部416は、新しいCA情報B301bが取得された後は、上記と同様に、CA情報B301bを用いてアプリケーションサーバ401の認証を行う。

#### 【0076】

以降、CA証明書の有効期限が近づいたときには、同様の動作を行うことにより、クライアント415は自動的に新しいCA証明書を取得できるようになり、またCA証明書の有効期限が切れたときには自動的に新しいCA証明書を用いた認証を行えるようになる。

#### 【0077】

以上のように、本実施の形態によれば、認証局A101aは、CA証明書とペアで、次回にCA証明書をダウンロードするためのダウンロードサーバB406bのURLをクライアント415に送付しておく。そして、CA証明書の有効期限が近づくと、新しいCA証明書を発行する認証局B101bを稼働させ、同時に、ダウンロードサーバB406bを稼働させる。一方、クライアント415は、定期的にダウンロードサーバB406bのURLにアクセスを試み、アクセスに成功すれば、新しいCA証明書をダウンロードし、予備メモリ419に保存する。そして、通信相手のアプリケーションサーバ401のサーバ証明書が現在のCA証明書で認証できなくなった場合には、予備メモリ419に保存されている新しいCA証明書で認証し、アプリケーションサーバの正当性を確認できれば、元のCA証明書を削除し、以降は新しいCA証明書をサーバ証明書の認証に使用する。

#### 【0078】

これによって、クライアント415は、次に有効となるCA証明書を保持するだけでCA証明書を更新することができるので、常に多数個のCA証明書を保有したり、複数のCA証明書を用いて検証するプログラムもしくは回路を組み込んでおいたりする必要がない。また、クライアント415は、定期的にダウンロードサーバB406bにアクセスして新しいCA証明書を取得することで、新たに

アプリケーションサーバとの通信を開始することができるので、時計を用いてCA証明書の有効期限を監視する必要がない。よって、クライアント415は、家電製品などのように十分なリソースを保有していない機器であっても、CA証明書の有効期限がいつかを気にすることなく、確実にCA証明書の取得および更新を行うことができる。

#### 【0079】

なお、CA情報更新部417が、メモリ418に保存されているCA情報に記載されているURLが示すダウンロードサーバへの接続は1ヶ月毎に試みるとしたが、1ヶ月ではなくそれより長いもしくは短い期間であってもよい。またその期間は均一であってもよいし、ある程度ばらついていても構わない。要するに、ダウンロードサーバの稼働開始から現在のCA証明書の有効期限が切れる間に確実に1度は接続を試みられる期間であればよい。

#### 【0080】

またアプリケーションサーバ401は、CA証明書の有効期限が切れると同時に、新しいAPサーバ公開鍵とAPサーバ秘密鍵の鍵ペアを作成するとしたが、CA証明書の有効期限内でも新しいAPサーバ公開鍵とAPサーバ秘密鍵の鍵ペアを作成し、新しいAPサーバ証明書を取得してもよい。この場合でも新しいAPサーバ証明書には、同じCA秘密鍵によるAP署名が含まれているので、クライアント415は保存しているCA公開鍵を用いて新しいAPサーバ証明書の認証を行うことができる。

#### 【0081】

また、図1のCA情報301にその他の情報が含まれていても構わない。

#### 【0082】

また、CA情報更新部417は、ダウンロードした新しいCA情報の正当性が確認できると、新しいCA情報を予備メモリ419に保存するが、このときCA署名303は保存しなくてもよい。これにより予備メモリ419の容量を削減可能となる。

#### 【0083】

同様に、初期状態としてメモリ418にはCA情報A106aが保存されてい

るが、CA署名A303aは保存しておかなくてもよい。

#### 【0084】

また、サーバ認証部416は、予備メモリ419に保存されているCA情報106bをメモリ418に保存し、予備メモリ419を空にするとしたが、その代わりにメモリ418を空にして、それ以降はメモリ418と予備メモリ419の役割を交代させるようにし、以降CA情報の更新を行う毎に、メモリ418と予備メモリ419の役割を交代させるようにしてもよい。

#### 【0085】

さらに、本発明のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体も本発明に属する。

#### 【0086】

さらに、本発明のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体も本発明に属する。

#### 【0087】

##### （第2の実施の形態）

以下、本発明の第1の実施の形態における認証局およびダウンロードサーバの運用の一例を、本発明の第2の実施の形態として、図3～図7を用いて説明する。

#### 【0088】

図3は、認証局およびダウンロードサーバの運用例を表すフローチャートである。

#### 【0089】

図4は、ダウンロードサーバの終了判断を行うフローチャートである。

#### 【0090】

図5は、正常時の認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例である。

**【0091】**

図6は、CA証明書Aが有効期限前に失効した場合の認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例で、失効時に次回ダウンロードサーバが未稼働の場合である。

**【0092】**

図7は、CA証明書Aが有効期限前に失効した場合の認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例で、失効時に次回ダウンロードサーバがすでに稼働している場合である。

**【0093】**

本実施の形態においては、CA情報301を発行し、かつアプリケーションサーバ401にAPサーバ証明書を発行する装置を、認証局と表記する。

**【0094】**

また、CA証明書A106aの有効期限を20年とし、CA証明書A106aの有効期限が切れる5年前に新しい認証局B101bおよびダウンロードサーバB406bを稼働させるものとする。

**【0095】**

またダウンロードサーバは、一つ前のCA証明書に指定されている有効期限が切れる時に稼働を終了させるものとする。例えば、ダウンロードサーバB406bは、CA証明書A106aに指定されている有効期限、すなわち認証局A101aの稼働開始から20年後となる。

**【0096】**

まず認証局およびダウンロードサーバの運用例を図3および図4のフローチャートを用いて説明する。

**【0097】**

図3において、ステップ501で運用を開始、ステップ502で認証局A101aの稼働を開始する。

**【0098】**

ステップ503でCA証明書A106aが有効期限前に失効しているかどうかを確認し、失効している場合にはステップ511に、失効していない場合にはス

ステップ504に進む。

#### 【0099】

ステップ504でCA証明書A106aの有効期限が切れる5年前になつてゐるかどうかを確認し、5年前になつてない場合にはステップ503に戻り、5年前になつた場合にはステップ505に進む。

#### 【0100】

ステップ505で認証局B101bを仮稼働させ、ステップ506でダウンロードサーバB406bを稼働させ、ステップ507に進む。この時点では、認証局B101bはCA公開鍵BとCA秘密鍵B105bとの鍵ペアを作成し保有しているが、アプリケーションサーバ401がクライアント415に送付するサーバ証明書はAPサーバ証明書A402aのままである。

#### 【0101】

ステップ507でCA証明書A106aが有効期限前に失効しているかどうかを確認し、失効している場合にはステップ509に、失効していない場合にはステップ508に進む。

#### 【0102】

ステップ508でCA証明書A106aの有効期限が切れているかどうかを確認し、切れていない場合にはステップ507に戻り、切れた場合にはステップ509に進む。

#### 【0103】

ステップ509で認証局A101aの稼働を終了させ、ステップ510で認証局B101bを本稼働させ、ステップ512に進む。この時点で、アプリケーションサーバ401がクライアント415に送付するサーバ証明書は、CA秘密鍵B105bによる署名が付加されたAPサーバ証明書Bである。

#### 【0104】

ステップ511ではダウンロードサーバ406bを稼働させ、ステップ509に進む。

#### 【0105】

ステップ512に進むと、ステップ503に戻り、AおよびaをBおよびbに

、BおよびbをCおよびcにそれぞれ置き換えて、ステップ503以降の動作を実行する。

#### 【0106】

また現在稼働しているダウンロードサーバの稼働を終了させるかどうかは、図4に示すフローチャートで表される。

#### 【0107】

ステップ601でダウンロードサーバが稼働すると、ステップ602でダウンロードサーバの稼働期間を確認し、稼働期間を終了していない場合は、ステップ602に戻り稼働期間の終了まで待ち、稼働期間を終了している場合は、ステップ603に進む。

#### 【0108】

ステップ603でダウンロードサーバの稼働を終了し、ステップ604で終了する。

#### 【0109】

以降、同様の動作を繰り返し、認証局およびダウンロードサーバの稼働と終了を行う。

#### 【0110】

以上のように、本実施の形態によれば、CA証明書が有効期限で終了した場合だけでなく、有効期限前に失効した場合であっても、実施の形態1と同様に、クライアント415は、次に有効となるCA証明書を保持するだけでCA証明書を更新することができるので、常に多数個のCA証明書を保有したり、複数のCA証明書を用いて検証するプログラムもしくは回路を組み込んでおいたりする必要がない。また、クライアント415は、定期的に、次に有効となるダウンロードサーバにアクセスして新しいCA証明書を取得することで、新たなアプリケーションサーバとの通信を開始することができるので、時計を用いてCA証明書の有効期限を監視する必要がない。よって、クライアント415は、家電製品などのように十分なリソースを保有していない機器であっても、CA証明書の有効期限がいつかを気にすることなく、確実にCA証明書の取得および更新を行うことができる。

### 【0111】

なお図3において、ステップ505とステップ506の順序は逆でもよいし、全く同時であっても構わない。同様にステップ509とステップ510の順序は逆でもよいし、全く同時であっても構わない。

### 【0112】

次に図3および図4のフローチャートに従って認証局およびダウンロードサーバの運用を行った場合の、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローを、通常時（CA証明書が有効期限切れにより失効）、および有効期限切れより前に何らかの理由でCA証明書が失効したときのそれぞれの場合について説明する。なお有効期限切れより前に何らかの理由でCA証明書が失効した場合の動作フローは、失効した時点で次のダウンロードサーバが稼働しているときと、稼働していないときの2通りについて説明する。

### 【0113】

図5は通常時のクライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローである。

### 【0114】

初期状態のクライアント415においては、メモリ418内にはCA情報A301aが保存されているが、予備メモリ419には何も保存されていない。

### 【0115】

CA証明書A106aの有効期限内は、アプリケーションサーバ401が送付するAPサーバ証明書AはCA公開鍵Aで認証可能であるため、クライアント415は自身が保持しているCA情報A301aを用いてアプリケーションサーバ401の正当性を確認できる。

### 【0116】

またクライアント415は、URL B302bが示すダウンロードサーバB406bへの接続を定期的に試みるが、CA証明書A106aの有効期限が切れる5年前まではダウンロードサーバB406bはまだ稼働していないため、接続には必ず失敗する。

### 【0117】

CA証明書A106aの有効期限が残り5年前になった時点で、新しい認証局B101bを稼働し、新しいCA証明書B106bとCA情報B301bが作成される。同時にCA情報B301bのダウンロードが可能なダウンロードサーバ406bを稼働する。

#### 【0118】

ダウンロードサーバ406bが稼働すると、クライアント415は、ダウンロードサーバ406bへの接続に成功し、CA情報B301bを取得することができる。クライアント415は、CA情報B301bが正当であることを確認すると、CA情報B301bを予備メモリ419に保存する。

#### 【0119】

クライアント415は、ダウンロードサーバ406bへの接続を定期的に試みるため、CA証明書A106aの有効期限が切れる前は、CA情報B301bを取得した後であってもダウンロードサーバ406bへの接続とCA情報B301bの取得は継続される。この場合、予備メモリ419内のCA情報と取得したCA情報が同一であれば予備メモリ419への保存をしないようにしてもよいし、取得したCA情報が正当なものであれば常に上書きするようにしてもよい。

#### 【0120】

さてCA証明書A106aの有効期限が切れると、アプリケーションサーバ401は、新しいCA証明書B106bで認証するAPサーバ証明書Bを、サーバ認証に用いるようになる。この後、クライアント415がアプリケーションサーバ401とのSSL通信を開始するにあたり取得するサーバ証明書はAPサーバ証明書Bになるが、保持しているCA証明書A106aではAPサーバ証明書Bの認証は失敗する。

#### 【0121】

すると、クライアント415は予備メモリ419に保存しているCA情報B301b内のCA証明書B106bを用いてAPサーバ証明書Bの認証を行う。クライアント415は、APサーバ証明書Bが正当であると確認すると、SSL通信を継続し、同時に予備メモリ419内のCA情報B301bをメモリ418に移し、予備メモリ419内の情報は削除する。

**【0122】**

これ以降、クライアント415は、CA証明書B106bを用いてサーバ認証を行い、またCA情報B301b内のURL C302cで表されるダウンロードサーバCへの接続を定期的に行うようとする。

**【0123】**

この場合、ダウンロードサーバB406bは、CA証明書106aが失効すると同時に稼働を終了する。

**【0124】**

以下、同様の動作を継続することにより、認証局およびCA証明書が新しくなった場合でも、クライアント415はアプリケーションサーバ401の認証やCA証明書の更新を行えるようになる。

**【0125】**

さて、CA秘密鍵A105aが解読されるなど、CA秘密鍵A105aの安全性が保証できなくなった場合には、速やかにCA証明書A106aを失効させると同時に、新しい認証局B101bを稼働させ、新しいCA証明書B106bを発行する。同時にアプリケーションサーバ401は、新しい認証局B101bから新しいAPサーバ証明書Bを発行してもらい、サーバ認証に用いるようにしなければならない。

**【0126】**

図6は、次回のCA情報をダウンロードするためのダウンロードサーバが稼働する前に、現在のCA証明書が失効した場合の、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローである。

**【0127】**

CA証明書A106aが失効する前の各動作は、図5と同様である。

**【0128】**

CA証明書A106aが失効した時点で、認証局B101bはまだ稼働していないので、速やかに新しい認証局B101bを稼働し、新しいCA証明書B106bを発行すると同時に、CA情報B301bを作成する。またこれと同時にダウンロードサーバB406bを稼働させ、CA情報B301bをダウンロードで

きるようになる。

#### 【0129】

CA証明書A106aが失効した後、たまたまクライアント415がアプリケーションサーバ401のサーバ認証を行う前に、ダウンロードサーバB406bへの接続が成功し、新しいCA情報B301bを取得できた場合には、クライアント415は通常動作時と同様にCA情報の更新を行うことができる。

#### 【0130】

しかしCA情報B301bの取得前に、クライアント415がアプリケーションサーバ401のサーバ認証を行うと、クライアント415がAPサーバ証明書Bの認証に失敗するが、このとき予備メモリ419には新しいCA情報B301bは保存されていない。この場合、クライアント415はただちにダウンロードサーバB406bへの接続を試みる。この時点ではすでにダウンロードB406bが稼働しているので、クライアント415はダウンロードB406bから新しいCA情報B301bを取得できる。

#### 【0131】

新しいCA情報B301bを取得した後は、通常時と同様の動作を繰り返す。ただし図6に示すように、CA証明書A106aが有効期限前に失効した場合でも、ダウンロードサーバB406bは、CA証明書A106aの本来の有効期限であった時点まで稼働を継続する。

#### 【0132】

また図7は、次回のCA情報をダウンロードするためのダウンロードサーバが稼働した後に、現在のCA証明書が失効した場合の、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローである。

#### 【0133】

CA証明書A106aが失効する前の各動作は、図5と同様である。

#### 【0134】

CA証明書A106aが失効した時点で、アプリケーションサーバ401は新しい認証局B101bから発行された新しいAPサーバ証明書Bを、クライアント415とのサーバ認証に使用する。

### 【0135】

またCA証明書A106aが失効した時点で、認証局B101bおよびダウンロードサーバB406bは稼働しているので、クライアント415はCA情報B301bを取得できるようになっている。そのため、クライアント415がすでにCA情報B301bを取得し、予備メモリ419に保存していた場合には、図5と同様に、APサーバ証明書Bの認証に失敗した時点でCA情報の更新を行うことができる。

### 【0136】

またクライアント415はCA情報B301bを取得する前に、APサーバ証明書Bの認証に失敗した場合には、図6と同様にその時点でダウンロードサーバB406bに接続し、新しいCA情報B301bの取得を行い、APサーバ証明書Bの認証を継続する。

### 【0137】

それ以降は、通常時と同様の動作を繰り返す。ただし図7に示すように、CA証明書A106aが有効期限前に失効した場合でも、ダウンロードサーバB406bは、CA証明書A106aの本来の有効期限であった時点まで稼働を継続する。

### 【0138】

以下、同様の動作を継続することにより、CA証明書が有効期限前に失効した場合でも、クライアント415はアプリケーションサーバ401の認証やCA証明書の更新を行えるようになる。

### 【0139】

なお、CA証明書の有効期限を20年、CA証明書の有効期限が切れる5年前に新しい認証局およびダウンロードサーバを稼働させるとしたが、有効期限は20年でなくてもよく、また認証局およびダウンロードサーバの稼働開始はCA証明書の有効期限の5年前でなくてもよい。またCA証明書の有効期限は、全て20年である必要はなく、CA証明書ごとに異なっていてもよい。

### 【0140】

また、予備メモリ419に保存されているCA情報106bをメモリ418に

保存し、予備メモリ419を空にするとしたが、その代わりにメモリ418を空にして、それ以降はメモリ418と予備メモリ419の役割を交代させるようにし、以降CA情報の更新を行う毎に、メモリ418と予備メモリ419の役割を交代させるようにしてもよい。

### 【0141】

#### 【発明の効果】

以上説明したところから明らかなように、本発明は、リソースの少ない機器でも、CA証明書の有効期限がいつかを気にすることなく、確実にCA証明書の取得および更新を行うことが可能なサーバ認証装置、認証局およびダウンロードサーバの運用方法、媒体及び情報集合体を容易に提供することができる。

#### 【図面の簡単な説明】

##### 【図1】

第1の実施の形態におけるCA情報の一例を示す図

##### 【図2】

第1の実施の形態におけるサーバ認証を行うクライアントの構成例を示す図

##### 【図3】

第2の実施の形態における認証局およびダウンロードサーバの運用例を表すフローチャート

##### 【図4】

第2の実施の形態におけるダウンロードサーバの終了判断を行うフローチャート

##### 【図5】

第2の実施の形態における認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例（正常時）

##### 【図6】

第2の実施の形態における認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例（認証局B稼働前にCA証明書Aが期限前に失効）

##### 【図7】

第2の実施の形態における認証局、クライアント、ダウンロードサーバおよび  
アプリケーションサーバの動作フローの一例（認証局B稼働中にCA証明書Aが  
期限前に失効）

【図8】

SSLにおける鍵情報および証明書の準備を表す図

【図9】

SSLにおける通信プロトコルを表す図

【符号の説明】

101 認証局

101a 認証局A

101b 認証局B

102 クライアント

103 サーバ

104 CA公開鍵

105 CA秘密鍵

105a CA秘密鍵A

105b CA秘密鍵B

106 CA証明書

106a CA証明書A

106b CA証明書B

107 サーバ公開鍵

108 サーバ秘密鍵

109 サーバ証明書

110 署名

201 通信用共通鍵

301 CA情報

301a CA情報A

301b CA情報B

302 次回ダウンロードサーバのURL

302b ダウンロードサーバBのURL

302c ダウンロードサーバCのURL

303 CA署名

303a CA署名A

303b CA署名B

401 アプリケーションサーバ

402a APサーバ証明書A

403a APサーバ公開鍵A

404a APサーバ秘密鍵A

405a AP署名A

406b ダウンロードサーバB

408b DLサーバ証明書B

409b DLサーバ公開鍵B

410b DLサーバ秘密鍵B

412b DL署名B

413 DL秘密鍵

414 DL公開鍵

415 クライアント

416 サーバ認証部

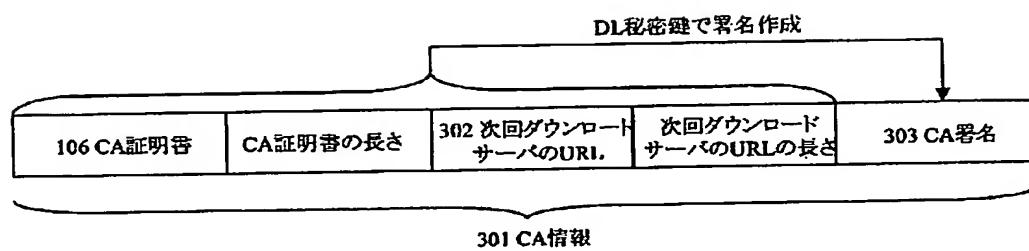
417 CA情報更新部

418 メモリ

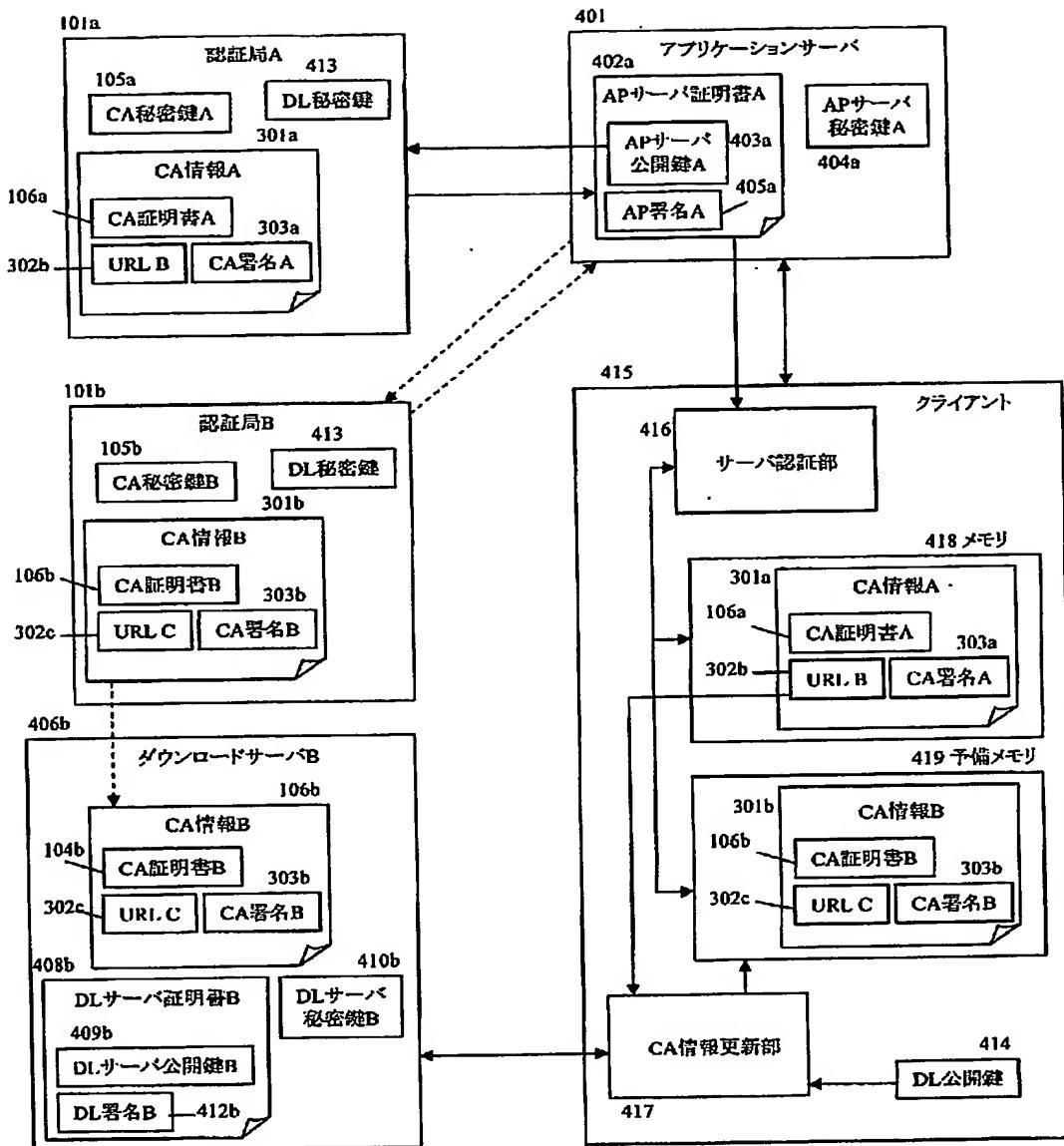
419 予備メモリ

【書類名】 図面

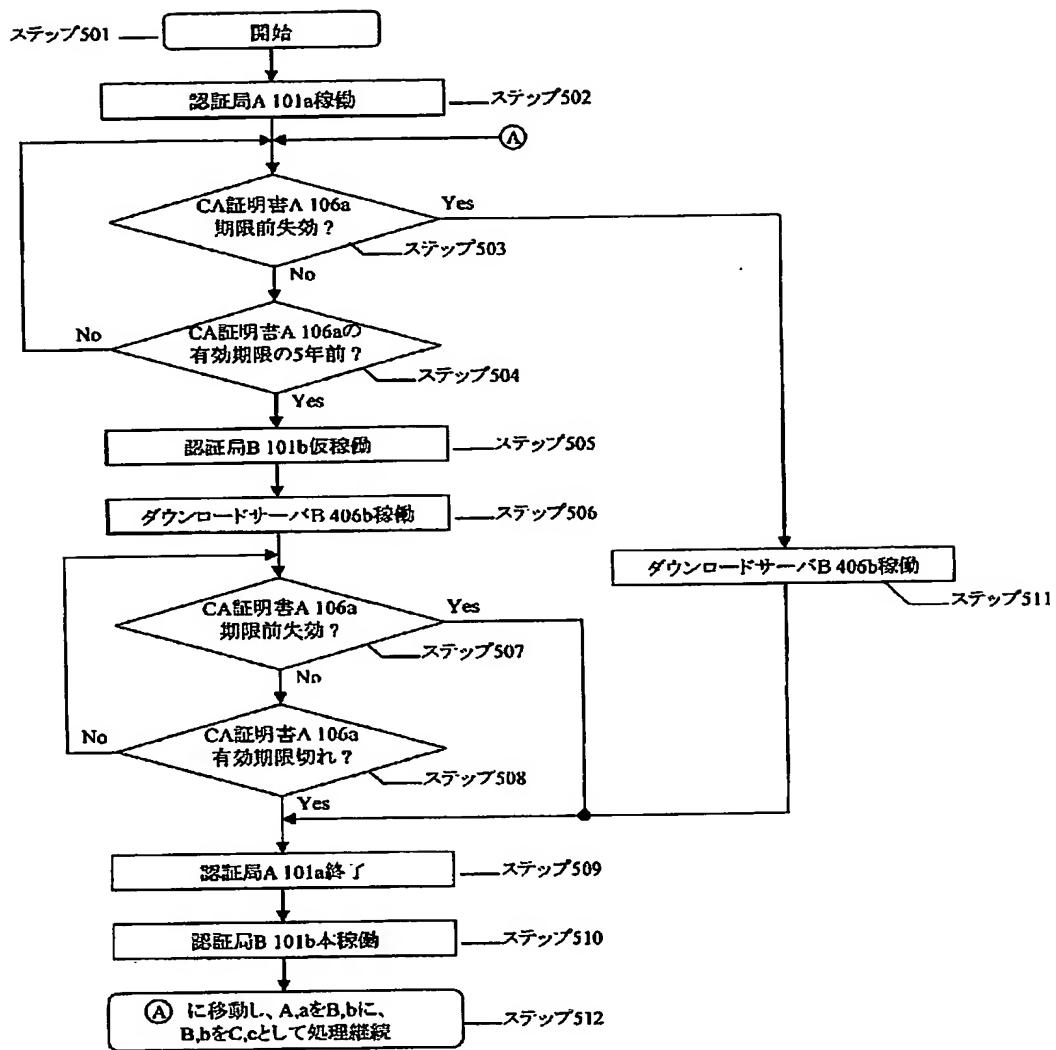
【図 1】



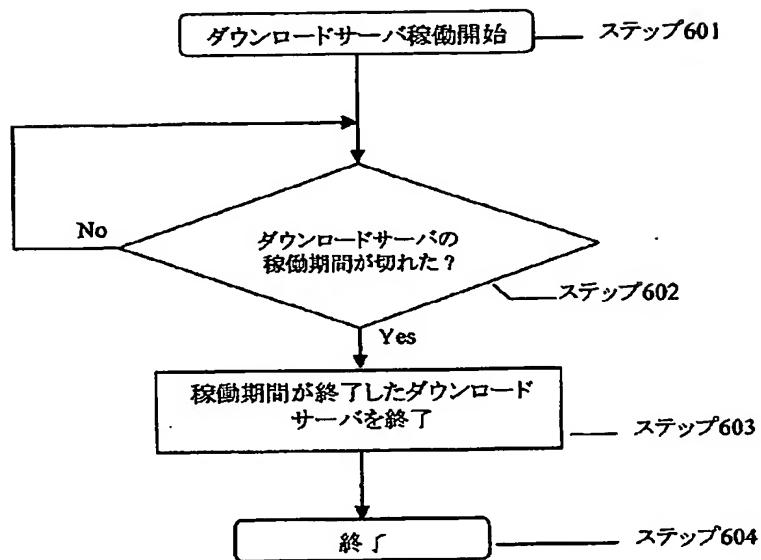
【図 2】



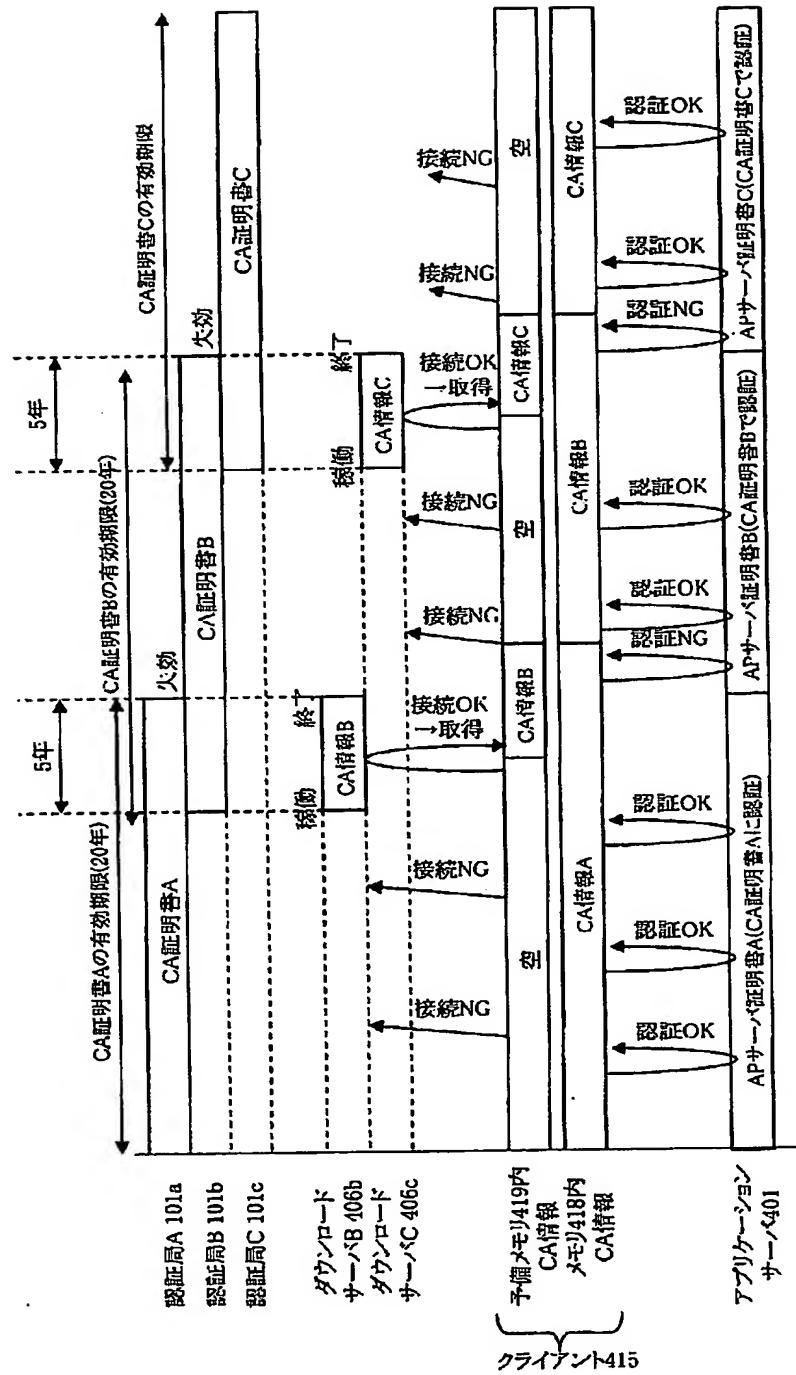
【図3】



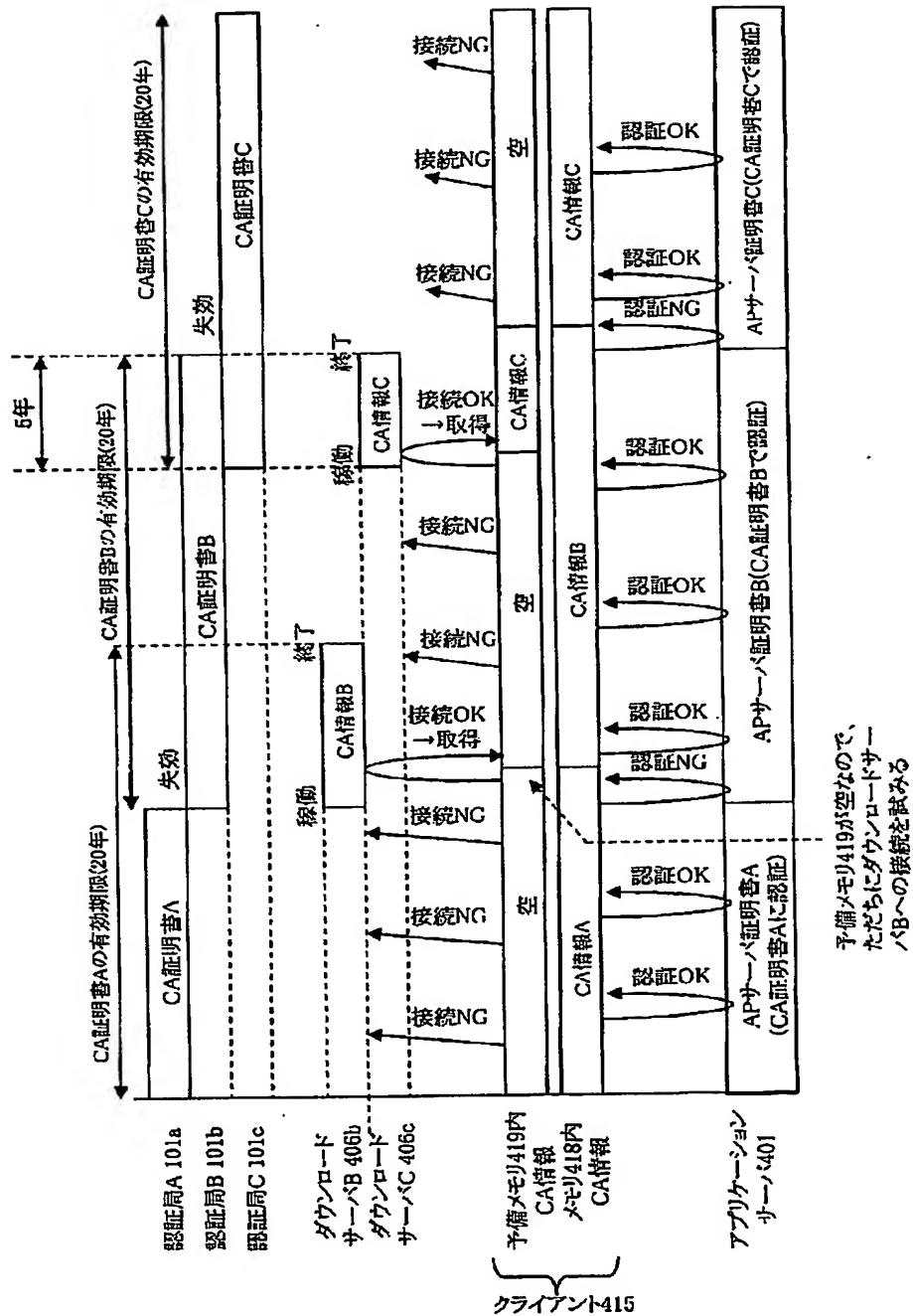
【図4】



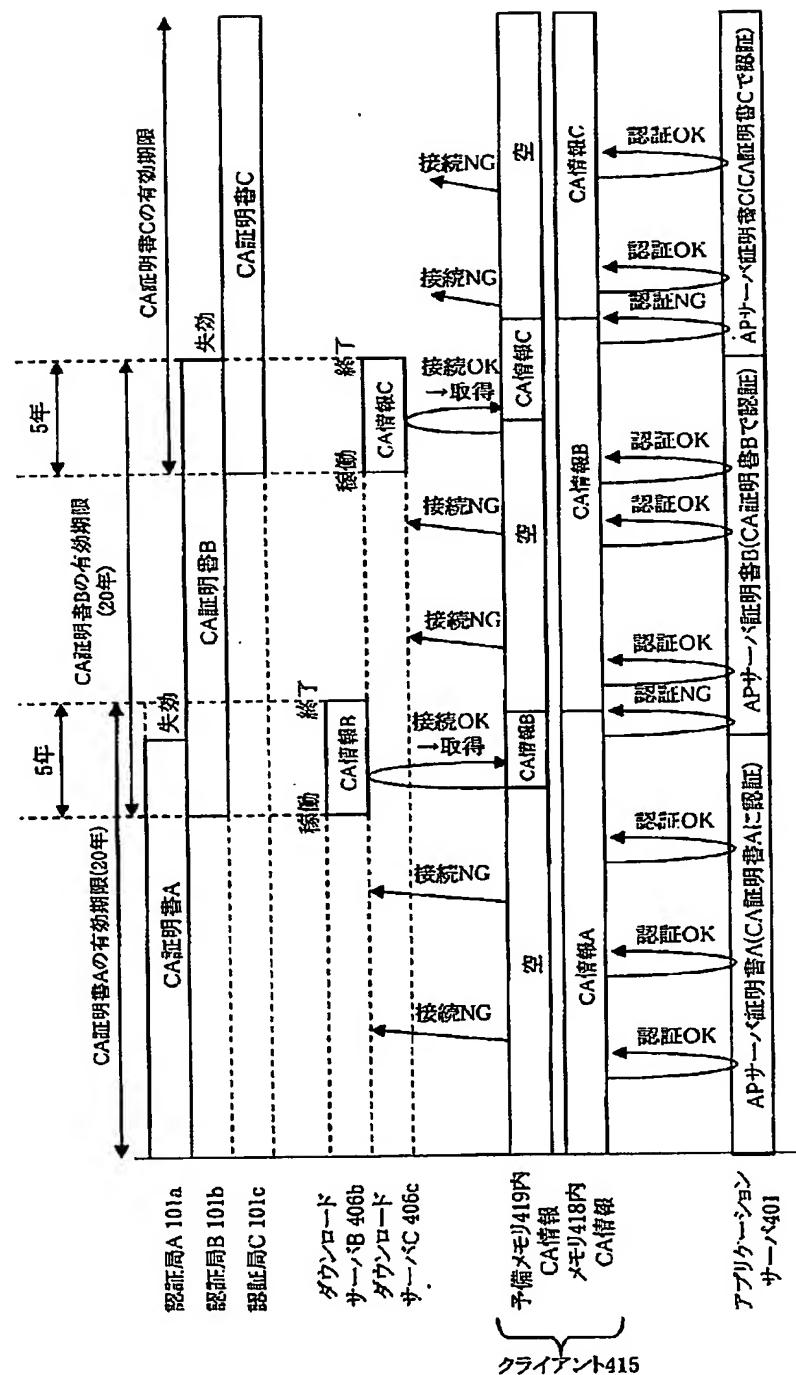
【图 5】



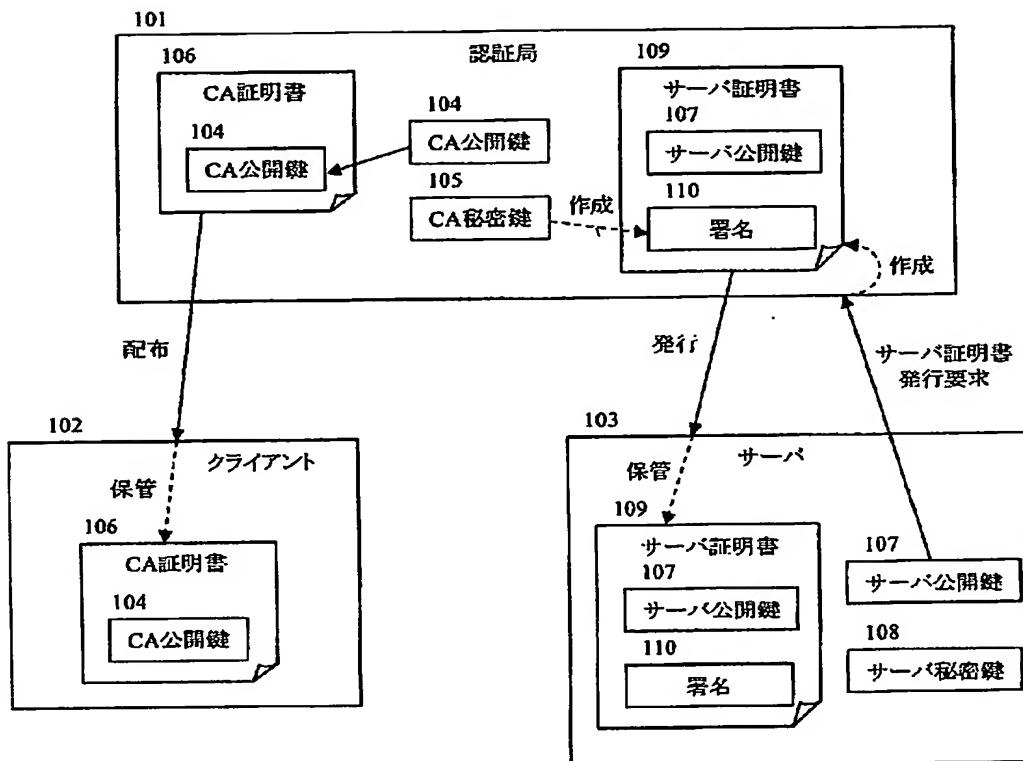
【図6】



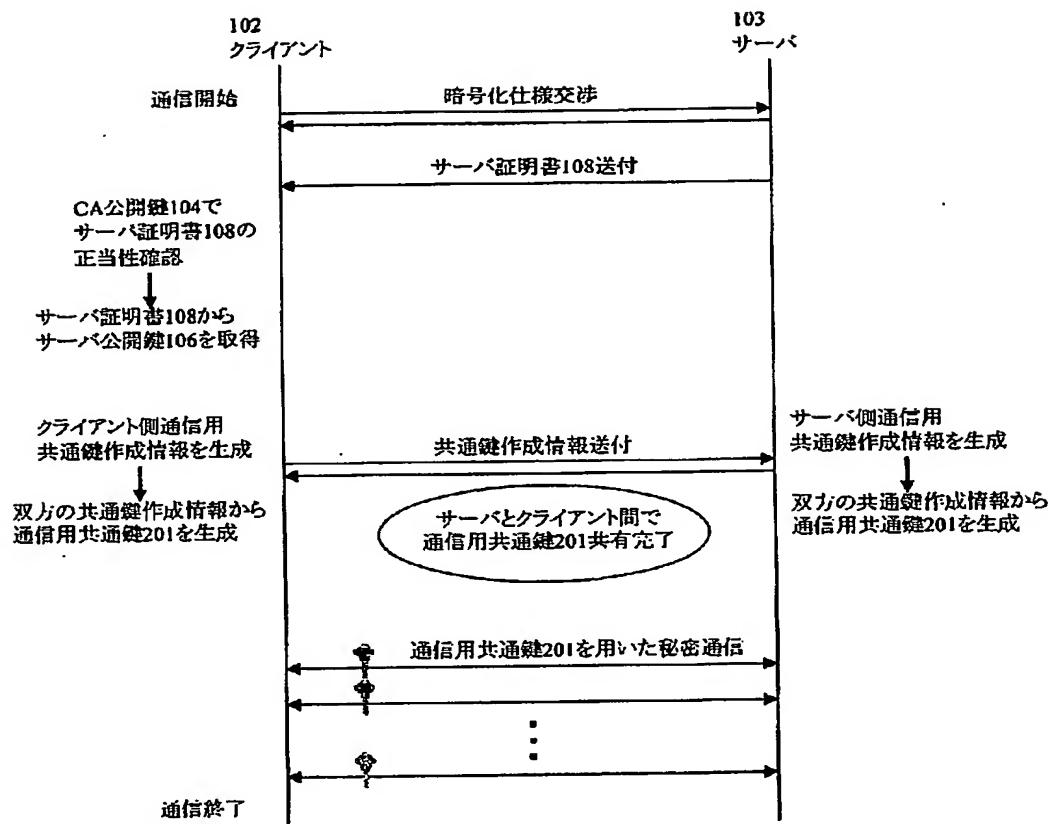
【図 7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】 リソースの少ないクライアントであっても安全かつ確実に新しいCA証明書を更新することができる認証局等を提供する。

【解決手段】 認証局A101aは、CA証明書とペアで、次回にCA証明書をダウンロードするためのダウンロードサーバB406bのURLをクライアント415に送付しておく。CA証明書の有効期限が近づくと、新しいCA証明書を発行する認証局B101bを稼働させ、同時に、ダウンロードサーバB406bを稼働させる。クライアント415は、定期的にダウンロードサーバB406bのURLにアクセスを試み、アクセスに成功すれば、新しいCA証明書をダウンロードし、予備メモリ419に保存しておき、アプリケーションサーバ401のサーバ証明書が現在のCA証明書で認証できなくなった場合に、予備メモリ419に保存していた新しいCA証明書で認証する。

【選択図】 図5

## 認定・付加情報

特許出願の番号 特願 2003-098596  
受付番号 50300545509  
書類名 特許願  
担当官 第八担当上席 0097  
作成日 平成15年 4月 4日

## &lt;認定情報・付加情報&gt;

【提出日】 平成15年 4月 1日

次頁無

出証特 2004-3031786

特願 2003-098596

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住所 大阪府門真市大字門真1006番地  
氏名 松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**